REMARKS

Claims 1-45 remain pending in the Application. Claims 1-45 stand rejected by the Examiner. Applicant traverses the rejections of claims 1-45.

Drawings

The drawings were objected to because figures 3, 4, and 5 were mislabeled. This response includes figures 3, 4, and 5 that have been corrected accordingly. Because Applicant has corrected the drawings to address these objections, Applicant respectfully submits that the objections to the drawings be removed and this application proceed to issuance.

Specification

The disclosure was objected to because of an informality. Because Applicant has corrected the specification to address this objection, Applicant respectfully submits that the objection to the specification be removed and this application proceed to issuance.

Claim Rejections

Claims 1-10, 16-25, 31-38 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Vanstone et al. U.S. Patent No. 6,122,736 (hereinafter the "Vanstone reference"). Claims 11-15, 26-30, 41-45 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the Vanstone reference and further in view of Heer U.S. Patent No. 6,028,933 (hereinafter the "Heer reference"). Applicant traverses these rejections.

Claim 1 recites that a plaintext message is encrypted into a ciphertext message and in the encrypting step, an ephemeral key pair is produced. That ephemeral key pair is then used in signing

a digital signature. The Examiner maintains that the Vanstone reference discloses at 3:7-9 and 3:49-53 the encryption of the plaintext message into a ciphertext message wherein the encrypting step includes the step of producing an ephemeral key pair; and further discloses signing a digital signature using the ephemeral key pair at 5:6-8.

Applicant respectfully disagrees with the Examiner's position. The Vanstone reference requires first performing the specific signing operation (at 3:7-9 and 5:6-8) *before* performing the encryption operation that "convert[s] plaintext ... into ciphertext" (at 3:49-53). Because Vanstone's encryption operation disclosed at 3:49-53 occurs *after* the signing operations, the signing operations *could not* use a key pair (let alone an ephemeral key pair) produced through Vanstone's encryption operation as required by claim 1. Accordingly, the Vanstone reference does not anticipate claim 1, and claim 1 is allowable.

The other independent claims (e.g., claims 16 and 31) are directed to encrypting a plaintext message into a ciphertext message and in the encrypting step, an ephemeral key pair is produced. That ephemeral key pair is then used in signing a digital signature. As shown above, the Vanstone reference does not disclose these limitations. Accordingly, claims 16 and 31 are allowable. Because each of the pending independent claims are allowable, their respective dependent claims are also allowable.

Applicant also disagrees with other positions presented by the Examiner. For example, claim 3 is allowable over the Vanstone reference. Claim 3 recites in combination with its other limitations that the generation of the digital signature includes hashing the plaintext message. The Vanstone reference does not disclose generating a signature based upon hashing a plaintext message. Accordingly, claim 3 is allowable for this additional reason over the Vanstone reference.

Applicant notes that claims 39 and 40 were not addressed by the Examiner and respectfully

requests that if a subsequent office action should issue, then such office action should address these claims as well.

CONCLUSION

For the foregoing reasons, Applicant submits that claims 1-45 are allowable. Therefore, the Examiner is respectfully requested to pass this case to issue.

Respectfully submitted,

Date: April 13, 2004

By: _____

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939